

**NIWC PACIFIC CODE 70000 TECHNICAL AND ENGINEERING SUPPORT  
SERVICES FOR THE CHIEF TECHNOLOGY OFFICE  
STATEMENT OF WORK (SOW) FOR SEAPORT-E NXG  
29 September 2022**

## **1.0 INTRODUCTION**

The Naval Information Warfare Center Pacific (NIWC Pacific) Science and Technology (S&T) Department, Code 70000, serves as NAVWAR's Chief Technology Office (CTO) to enhance Science and Technology development and facilitate efficient technology transition into acquisition programs. The CTO has a requirement for technical and engineering services to support its role in developing and transitioning technologies that meet the highest priority needs of the warfighter.

1.1 *Scope.* The objective of this Task Order is to obtain technical and engineering services to assist and support the NAVWAR CTO in carrying out its duties and responsibilities to develop world-class technologies in the areas of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR), cyber and space that support warfighter requirements. The Task Order requires skill sets that span subject matter expertise to graphic support services for CTO functions, which includes providing:

- S&T project and program management support services
- Technology Transition support services into Team NAVWAR product lines
- Technology Readiness Assessment (TRA) training and support within Team NAVWAR
- Technology Transfer (T2) support services
- Support services for the execution of Cooperative Research and Development Agreements (CRADAs)
- Qualitative research on strategic S&T investments that support the Navy's strategy for Information Warfare
- Technology experimentation support for laboratory and operational experiments
- Support Services for database tools tracking S&T projects across Team NAVWAR
- S&T portfolio investment support services for Command, Control, Communications, Computers and Intelligence (C4I) Communities of Interest (COI)

1.2 *Background.* The CTO at NIWC Pacific serves as the Technology Transition Agent, providing Technology Transfer services for Team NAVWAR, documenting transition categories, implementing transition data calls, establishing Technology Transition metrics, and teaming with industry, academia, and other Defense agencies to enhance technology speed and delivery for Naval capabilities. Technical and engineering support services will be used to assist the CTO in promoting S&T development throughout Team NAVWAR to fill warfighter needs and acquisition program gaps, and facilitating the rapid, efficient, and affordable transition of advanced technologies into new warfighting capabilities.

## **2.0 APPLICABLE DIRECTIVES**

UNCLASSIFIED

The contractor shall adhere to the following documents in the performance of the technical requirements outlined in paragraph 3.0:

UNCLASSIFIED

## UNCLASSIFIED

<b>Document Type</b>	<b>No./Version</b>	<b>Title</b>	<b>SOW Para.</b>
Navy Instruction	N/A	Navy Strategy for Achieving Information Dominance 2013-2017	3.3, 3.7
Navy Strategy Guide	NOV 2012	Navy Cyber Power 2020	3.2, 3.3, 3.7, 3.10
Navy Instruction	N/A	Navy Information Dominance Corps Human Capital Strategy 2012-2017	3.3, 3.7
SPAWAR Notice	5450	SPAWAR Reorganization Notice 5430, SPAWARNOTE 5430, 25 SEPT 2007	3.5, 3.6, 3.10
Navy Memorandum	JAN 2012	DASN RDT&E CTO Tenets, 18 JAN 2012	3.2, 3.3
Navy Instruction	N/A	Navy Information Dominance Roadmap 2013-2028	3.3, 3.7
SPAWAR Instruction	N/A	SPAWAR Strategic Vision 2018-2027	3.8, 3.10
SPAWAR Instruction	5238.2A/5.0	SPAWAR CONOPS for S&T Forecasting, Investment and Transition	3.2, 3.4, 3.7, 3.9
SPAWAR Instruction	N/A	SPAWAR Commander's Guidance 2014	3.8
SSC Pacific Strategy Guide	N/A	SSC Pacific Strategy Map	3.2, 3.3, 3.6
DoD Instruction	N/A	Reliance 21 Operating Principles	3.10
DOD Manual	5200.01, Volume 1	DoD Information Security Program: Overview, Classification, And Declassification, Ch-2 28 July 2020	4.0, 7.0
DOD Manual	5200.01, Volume 2	DoD Information Security Program: Marking Of Classified Information, Ch-4 28 July 2020	4.0, 7.0

UNCLASSIFIED

## UNCLASSIFIED

DOD Manual	5200.01, Volume 3	DoD Information Security Program: Protection Of Classified Information, Ch-3 28 July 2020	4.0, 7.0
DOD Instruction	5200.48	Controlled Unclassified Information (CUI), 6 March 2020	4.0, 7.0
DOD Manual	5200.02	Procedures for the DoD Personnel Security Program (PSP) dtd Ch-1 29 October 2020	4.0, 7.0
DoD Manual	5220.32, Volumes 1	National Industrial Security Program: Industrial Security Procedures for Government Activities, 1 August 2018, Ch-2 10 December 2021	4.0, 7.0
	32 CFR Part 117	National Industrial Security Program, Operating Manual (NISPOM), 24 February 2021	4.0, 7.0
SECNAV Instruction	5510.30C	Department of Navy Personnel Security Program, 24 January 2020	4.0, 7.0
SECNAV Instruction	5510.36B	DON Information Security Program, 12 July 2019	4.0, 7.0
DoD Directive	5205.02E	DoD Operations Security (OPSEC) Program, 20 June 2012, Ch-1 11 May 2018	4.0, 7.0
OPNAVINST	F3300.53D	Navy Antiterrorism Program, 2 August 2021	4.0, 7.0
SPAWAR Instruction	3432.1	Operations Security Policy, 2 February 2005	4.0, 7.0

UNCLASSIFIED

NIWCPAC Instruction	5500.1C	Security Manual, Ch-1 25 September 2019	4.0, 7.0
------------------------	---------	--	----------

### 3.0 TECHNICAL REQUIREMENTS

The contractor shall provide technical and engineering services to assist and support the NAVWAR CTO in carrying out its duties and responsibilities to develop world-class C4ISR that supports warfighter requirements. Work in this task order will require a TS/SCI clearance. During performance of this tasking, the contractor will attend meetings and assist in the review and creation of reports and presentation materials that include TS/SCI information. All TS/SCI information shall be accessed via appropriate Government channels as outlined in the DD-254.

- 3.1 *General Support.* The contractor shall provide technical support for the consolidated database for Technology Transfers, Technology Transitions, Cooperative Research and Development Agreements (CRADAs). The contractor shall draft and distribute unmanned aircraft system (UAS) flight schedules on a weekly basis, coordinate UAS training visits, and update training jackets for NIWC Pacific UAS pilots and observers. The contractor shall perform technical writing and prepare technical input, documentation, presentations, reports, schedules, milestone charts, strategy plans and metrics, and related written products as required by the CTO per the deliverable schedule. (CDRL Data Items A001, A002, and A003)
- 3.2 *Science and Technology Management Support.* The contractor shall engage with Service Systems Command, the Office of Naval Research (ONR), the Defense Advanced Research Projects Agency (DARPA), Department of Defense (DoD) and Department of Navy (DoN) agencies and organizations, academia and industry to provide technical analysis to foster S&T initiatives and teaming. The contractor shall support CTO processes and events that identify solutions to S&T gaps provided by Program Executive Officer, Command, Control, Communications, Computers & Intelligence (PEO C4I), Program Executive Officer, Space Systems (PEO SS), and Program Executive Officer, Enterprise Information Systems (PEO EIS). The contractor shall leverage industry best practices that generate new ideas, and produce new technologies, processes, strategies and services to improve warfighter capabilities. Work performed in this section requires a TS/SCI clearance in order to review NIWC Pacific's outgoing RDT&E funding opportunity proposals which include information up to the SCI level. JWICS access will also be required in order to communicate with Government team members (CDRLs A001 and A002).
- 3.3 *Technology Transition Support.* The contractor shall support the CTO in identifying, developing, assessing and transitioning new C4ISR battle management concepts and technologies into Team NAVWAR product lines that enable the Navy's Information Warfare vision. The contractor shall identify appropriate transition programs and policies that enable successful and rapid transition of concepts and technologies into Team NAVWAR products, the role specific technologies will play in improving warfighter capabilities, and potential and existing external partnerships with industry, academia, and the acquisition community. The contractor shall develop and maintain metrics for team

NAVWAR in the areas of innovation and technology transition. (CDRLs A001 and A002). Work performed in this section requires a TS/SCI clearance in order to review NIWC Pacific's outgoing RDT&E funding opportunity proposals, which include information up to the SCI level. Work in this section also requires JWICS access in order to communicate with acquisition partners.

- 3.4 *Technology Readiness Assessment (TRA)*. The contractor shall support the CTO in implementing standardized procedures for conducting TRA within Team NAVWAR. The contractor shall support the TRA Panel Chair for Acquisition Categories (ACAT) I and II TRA and provide guidance and support to Team NAVWAR program offices for ACAT III and IV TRA. The contractor shall document and track Team NAVWAR TRA by participating in periodic top-level management meetings with the CTO to assess each program of record TRA status and to provide recommendations in setting priorities. (CDRLs A001 and A002). Work in this section requires a TS/SCI clearance in order to review test reports, technology performance results, technology performance limitations and shortcomings, and threat assessments, all of which include information up to the TS/SCI level.
- 3.5 *Technology Transfer (T2)*. The Contractor shall perform tasks in support of the Technology Transfer Program that include, but are not limited to, support of CRADAs and Patent License Agreements (PLAs) development. In the performance of such tasks, the Contractor may be given access to proprietary information submitted to the Government by non-Government businesses and organizations.
  - 3.5.1 The contractor shall support the Office of Research and Technology Applications (ORTA) in T2 functions through licensing of Government Intellectual Property (IP) to commercial portfolio management. The contractor shall process, distribute and manage royalty payments, maintain the T2 Patent database, maintain the IP license folders and assist in capturing T2 metrics. The contractor shall conduct market research on NIWC Pacific technologies and IP for commercialization potential, and develop reports and presentations for ORTA. The contractor shall interface and work with technology distribution channels, including but not limited to university MBA programs, DoD Partnership Intermediaries, and technology locators to develop marketing activities and material to support NIWC Pacific technologies, IP, and capabilities for T2. The contractor shall perform NIWC Pacific IP portfolio analysis and reporting functions to the ORTA, the T2 office, and the Federal Laboratory Consortium Far West Regional Coordinator. (CDRLs A001 and A002)
- 3.6 *Technology Transfer Cooperative Research and Development Agreement (CRADAs)*. The contractor shall support the execution of CRADAs and develop collaborative Research and Development (R&D) partnerships with NIWC Pacific Principle Investigators (PIs) and commercial and non-commercial entities. The contractor shall maintain and update metrics related to CRADAs. The contractor shall provide S&T portfolio analysis, management, and related administrative support for NIWC Pacific CRADAs and facilitate the execution of Limited Purpose CRADAs (LP-CRADAs). (CDRLs A001 and A002)

- 3.7 *Strategic Development and Commander's Guidance Goals.* The contractor shall employ qualitative research to make strategic recommendations that directly impact the actions and decisions made by the CTO on future technology investments in support of the Navy's strategy and roadmap for Information Warfare. The contractor shall monitor, assess and map the landscape of technology innovations and identify areas to increase intellectual capital within Team NAVWAR. The contractor shall oversee development, implementation, execution, and data analysis for S&T objectives that meet warfighter requirements. The contractor shall oversee performance measures and initiatives development, data collection and distribution, and gap analysis for S&T objectives. (CDRLs A001, A002, and A003). Work in this section requires a TS/SCI clearance as well as JWICS access in order to review and assist in the creation of the strategy roadmap, which includes discussions of technologies up to the TS/SCI level.
- 3.8 *Experimentation and Support.* The contractor shall support the CTO's corporate experimentation efforts by engaging key experiment partners within Department of Navy (DoN) and DoD on laboratory experiments, warfighter demonstrations, operational exercises, and war games. The contractor shall collect technical requirements from Team NAVWAR program offices and disseminate these to the S&T stakeholders in the interest of aligning near, mid, and far term S&T experimentation efforts with programmatic technology gaps and fleet requirements. The contractor shall maintain metrics for experimentation outcomes under the CTO adherence to the NAVWAR CONOPS for S&T Forecasting, Investment and Transition (CDRLs A001 and A002). Work in this section requires a TS/SCI clearance in order to review priority lists, which include information up to the TS/SCI level. The contractor will also be required to be attend and write status reports from Live Virtual and Constructive (LVC) experimentation environments, which contain information up to the TS/SCI level.
- 3.9 *CTO Outreach and Technology database tool support.* The contractor shall provide support for a variety of tools required by the CTO's office, including maintenance of the website content for technology transition proposal opportunities, the test and evaluation and maintenance of the informational outreach web site, the Science & Technology Alignment and Investment Reporting System (STAIRS) or other similar database tools for tracking S&T projects across the NAVWAR claimancy and agencies supported by NAVWAR. The contractor shall support the roll out of databases and similar tools to users in the NAVWAR claimancy and agencies supported by NAVWAR, training new users and developing training materials, and shall respond to user's questions via telephone and email. In addition, the contractor shall enter proposals, projects, publications, and patent records into the database and serve as curator of database content. The contractor shall support the analysis and integration of other potential data sharing tools.
- 3.10 *Command and Control, Communications, Computer, and Intelligence (C4I) Community of Interest (COI) Support.* The contractor shall provide technical and administrative support including:
- 3.10.1 Administrative support for preparation of presentation and meeting materials;  
coordination of meeting and workshop locations - both virtual collaboration spaces

and live meeting locations; the capture, consolidation and dissemination of meeting minutes; collection, management and maintenance of COI member contact information and meeting attendance; and support in the creation and maintenance of synchronous and asynchronous collaboration spaces. The contractor shall host one annual C4I COI-wide workshop, an all-hands meeting, and an industry technology-exchange forum.

3.10.2 Technical contributions that include continued refinement of the C4I Roadmap; research and summary of Joint, Army, Navy and Air Force doctrine relevant to C4I; development of Technology and Capability Working Groups' shell presentations, laying out the content and format of technology and capability roadmaps; development of the C4I Capability brief to the COI; preparation of a Joint C4I Roadmap from service specific roadmaps; examination and rollout of technology roadmaps; identification of technology gaps; and preparation of the final presentation format and content.

3.10.3 Support for working group tasks that include but are not limited to the following: Collect data and provide analysis and recommendations to support all C4I COI Steering Group functions. Provide a collaborative forum to bring forward C4I S&T issues, needs, capabilities, gaps, and concerns for discussion, resolution, or submission to the steering group as appropriate; Identify critical C4I S&T shortfalls; provide recommendations to the Steering Group for advocacy to the S&T EXCOM; Review strategic level technical objectives of DoD component S&T programs related to C4I; Review progress of DoD C4I projects on an annual basis and recommend to the S&T EXCOM, through the Steering Group, any needed changes in the activities, based on metrics and analyses to be established by the Steering Group, and report progress to the C4I Steering Group on an annual basis; and provide a coordination mechanism for DoD engagement with interagency C4I activities; Support the Steering Group in carrying out tasks as assigned; Establish subgroups with the consent of the Steering Group.

#### **4.0 CYBER SECURITY**

Cybersecurity (which replaced the term Information Assurance (IA)) is defined as prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Contractor personnel shall perform tasks to ensure Navy applications, systems, and networks satisfy Federal/DoD/DON/Navy cybersecurity requirements.

##### **Cyber IT and Cybersecurity Personnel**

(a) The Cyberspace workforce elements addressed include contractors performing functions in designated Cyber IT positions and Cybersecurity positions. In accordance with DFARS Subpart 239.71, DoDD 8140.01, SECNAVINST 5239.20A, and SECNAV M-5239.2, contractor personnel performing cybersecurity functions shall meet all cybersecurity training, certification, and tracking requirements as cited in DoD 8570.01-M prior to accessing DoD information

UNCLASSIFIED

systems. Proposed contractor Cyber IT and cybersecurity personnel shall be appropriately qualified prior to the start of the contract performance period or before assignment to the contract during the course of the performance period.

(b) The contractor shall be responsible for identifying, tracking and reporting cybersecurity personnel, also known as Cybersecurity Workforce (CSWF) and Cyber IT workforce personnel. Although the minimum frequency of reporting is monthly, the task order can require additional updates at any time.

(c) Contractors that access Navy IT shall also follow guidelines and provisions documented in Navy Telecommunications Directive (NTD 10-11) and are required to complete a System Authorization Access Request (SAAR) – Navy form as documented in para 8.2.2.4(b).

When a contractor requires logical access to a government IT system or resource (directly or indirectly), the required CAC will have a Public Key Infrastructure (PKI). A hardware solution and software (e.g., ActiveGold) is required to securely read the card via a personal computer. Pursuant to DoDM 1000.13-M-V1, CAC PKI certificates will be associated with an official government issued e-mail address (e.g., .mil, .gov, .edu). Prior to receipt of a CAC with PKI, contractor personnel shall complete the mandatory Cybersecurity Awareness training and submit a signed System Authorization Access Request Navy (SAAR-N) form to the contract's specified COR. Note: In order for personnel to maintain a CAC with PKI, each contractor employee shall complete annual cybersecurity training. The following guidance for training and form submittal is provided; however, contractors shall seek latest guidance from their appointed company Security Officer and the NIWC Pacific Information Assurance Management (IAM) office:

For annual DoD Cybersecurity/IA Awareness training, contractors shall use this site: <https://twms.nmci.navy.mil/>. For those contractors requiring initial training and do not have a CAC, contact the NIWC Pacific IAM office. Training can be taken at the IAM office or online at <http://iase.disa.mil/index2.html>.

For SAAR-N form, the contractor shall use OPNAV 5239/14 (Rev 9/2011). Contractors can obtain a form from the NIWC Pacific IAM office or from the website: <https://navalforms.documentservices.dla.mil/>.

(d) Contractor personnel with privileged access will be required to acknowledge special responsibilities with a Privileged Access Agreement (PAA) IAW SECNAVINST 5239.20A.

#### Design, Integration, Configuration or Installation of Hardware and Software

The contractor shall ensure any equipment/system installed or integrated into Navy platform will meet the cybersecurity requirements as specified under DoDI 8500.01. The contractor shall ensure that any design change, integration change, configuration change, or installation of hardware and software is in accordance with established DoD/DON/Navy cyber directives and does not violate the terms and conditions of the accreditation/authorization issued by the appropriate Accreditation/Authorization official. Contractors that access Navy IT are also required to follow the provisions contained in DON CIO Memorandum:

UNCLASSIFIED

## UNCLASSIFIED

Acceptable Use of Department of the Navy Information Technology (IT) dated 12 Feb 16. Use of blacklisted software is specifically prohibited and only software that is registered in DON Application and Database Management System (DADMS) and is Functional Area Manager (FAM) approved can be used as documented in para 5.2.2. Procurement and installation of software governed by DON Enterprise License Agreements (ELAs) – Microsoft, Oracle, Cisco, Axway, Symantec, ActivIdentity, VMware, Red Hat, NetApp, and EMC shall be in accordance with DON CIO Policy and DON ELAs awarded.

### Cybersecurity Workforce (CSWF) Report

DoD 8570.01-M and DFARS PGI 239.7102-3 have promulgated that contractor personnel shall have documented current cybersecurity certification status within their contract. The contractor shall develop, maintain, and submit a CSWF Report as applicable at the task order level. IAW DFARS clause 252.239-7001, if cybersecurity support is provided, the contractor shall provide a Cybersecurity Workforce (CSWF) list that identifies those individuals who are IA trained and certified. Utilizing the format provided at the task order level, the prime contractor shall be responsible for collecting, integrating, and reporting all subcontractor personnel. See applicable DD Form 1423 for additional reporting details and distribution instructions. Contractor shall verify with the COR or other government representative the proper labor category cybersecurity designation and certification requirements.

### Information Technology (IT) Services Requirements

This paragraph only applies to IT contracts. Information Technology (IT) is defined as any equipment or interconnected system(s) or subsystem(s) of equipment that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. IT includes computers, ancillary equipment, peripherals, input, output, and storage devices necessary for security and surveillance. Electronic and Information technology (EIT) is IT that is used in the creation, conversion, or duplication of data or information. EIT includes: telecommunication products, such as telephones; information kiosks; transaction machines; World Wide Web sites; multimedia (including videotapes); and office equipment, such as copiers and fax machines.

### Information Technology (IT) General Requirements

When applicable, the contractor shall be responsible for the following:

- Ensure that no production systems are operational on any RDT&E network.
- Follow DoDI 8510.01 of 12 Mar 2014 when deploying, integrating, and implementing IT capabilities.
- Migrate all Navy Ashore production systems to the NMCI environment where available.
- Work with government personnel to ensure compliance with all current Navy IT & cybersecurity policies, including those pertaining to Cyber Asset Reduction and Security (CARS).

UNCLASSIFIED

## UNCLASSIFIED

- Follow SECNAVINST 5239.3B of 17 June 2009 & DoDI 8510.01 of 12 Mar 2014 prior to integration and implementation of IT solutions or systems.
- Register any contractor-owned or contractor-maintained IT systems utilized on contract in the Department of Defense IT Portfolio Registry (DITPR)-DON.
- Only perform work specified within the limitations of the task order.

### Acquisition of Commercial Software Products, hardware, and Related Services

This paragraph only applies to the purchasing/hosting of commercial software. Contractors recommending or purchasing commercial software products, hardware, and related services supporting Navy programs and projects shall ensure they recommend or procure items from approved sources in accordance with the latest DoN and DoD policies.

### DON Enterprise Licensing Agreement/DOD Enterprise Software Initiative Program

Pursuant to DoN Memorandum – Mandatory use of DoN Enterprise Licensing Agreement (ELA) dated 22 Feb 12, contractors that are authorized to use Government supply sources per FAR 51.101 shall verify if the product is attainable through DoN ELAs and if so, procure that item in accordance with appropriate ELA procedures. If an item is not attainable through the DoN ELA program, contractors shall then utilize DoD Enterprise Software Initiative (ESI) program (see DFARS 208.74) and government-wide SmartBuy program (see DoD memo dated 22 Dec 05). The contractor shall ensure any items purchased outside these programs have the required approved waivers as applicable to the program. Software requirements will be specified at the task order level.

### DON Application and Database Management System

The contractor shall ensure that no Functional Area Manager (FAM) disapproved applications are integrated, installed or operational on Navy networks. The contractor shall ensure that all databases that use database management systems (DBMS) designed, implemented, and/or hosted on servers and/or mainframes supporting Navy applications and systems be registered in DoN Application and Database Management System (DADMS) and are FAM approved. All integrated, installed, or operational applications hosted on Navy networks must also be registered in DADMS and approved by the FAM. No operational systems or applications will be integrated, installed, or operational on the RDT&E network.

### Section 508 Compliance

This paragraph only applies to IT contracts. The contractor shall ensure that all software recommended, procured, and/or developed is compliant with Section 508 of the Rehabilitation Act of 1973, 26 CFR Part 1194 and pursuant to SPAWARINST 5721.1B of 17 Nov 2009. In accordance with FAR 39.204, this requirement does not apply to contractor acquired software that is incidental to the task, software procured/developed to support a program or system designated as a National Security System (NSS) or if the product is located in spaces frequented only by service personnel for maintenance, repair or occasional monitoring of equipment.

UNCLASSIFIED

## UNCLASSIFIED

### Software Development/Modernization and Hosting

This paragraph only applies to software development and modernization. The contractor shall ensure all programs utilizing this contract for software development/ modernization (DEV/MOD), including the development of IT tools to automate NIWC Pacific business processes are compliant with DON Information Management/Information Technology (DON IM/IT) Investment Review Process Guidance requirements. Contractors shall neither host nor develop IT tools to automate NIWC Pacific business processes unless specifically tasked within the task order or contract. The contractor shall ensure IT tools developed to automate NIWC Pacific business processes will be delivered with full documentation and source code, as specified at the task order level, to allow non-proprietary operation and maintenance by any source. The contractor shall ensure all programs are submitted with proof of completed DEV/MOD certification approval from the appropriate authority in accordance with DON policy prior to task order award. \*Note must be listed on Investment Review Board (IRB) approved list.

### Information Security

Pursuant to DoDM 5200.01 and DoD/DoD 5200.48, the contractor shall provide adequate security for all CUI and Unclassified DoD information passing through non-DoD information system including all subcontractor information systems utilized on contract. If the contractor originates, adds, or changes any of the DoD information, it must be marked in accordance with DODI 5200.48 and handled properly. The contractor shall disseminate CUI and unclassified DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the contractor, information developed during the course of the contract, and privileged contract information (e.g., program schedules, contract-related tracking).

### IT Position Designations

Pursuant to DoDI 8500.01, DoD 8570.01-M, SECNAVINST 5510.30, SECNAV M-5239.2, and applicable to unclassified DoD information systems, a designator is assigned to certain individuals that indicates the level of Special-Sensitive (SS)/Critical-Sensitive (CS) or Noncritical Sensitive (NCS), access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. Per SECNAVINST 5510.30C, page 7, Section 8.b of enclosure (4), the Information Systems Security Manager is responsible for establishing, implementing and maintaining the DoN information system and information assurance program and is responsible to the Commanding Officer for developing, maintaining, and directing the implementation of the Information Assurance (IA) program within the command. The three basic position sensitivity levels/Position Designations:

Special-Sensitive (SS)/T5 or T5R; equivalent (SSBI, etc.) (IT Level I) - Potential for inestimable impact and/or damage.

UNCLASSIFIED

## UNCLASSIFIED

Critical-Sensitive (CS)/T5 or T5R; equivalent (SSBI, etc.) (IT Level I) - Potential for grave to exceptionally grave impact and/or damage.

Noncritical Sensitive (NCS)/T3 or T3R; equivalent (ANAC/ANACI) (IT Level II) - Potential for some to serious impact and/or damage.

### **5.0 TRAVEL**

This task may require contractor travel to locations within the continental United States. The request for all routine travel in support of this task order shall be made via email to the COR no later than five (5) working days in advance of the anticipated travel date for final approval. For emergent travel, requests shall be made via email to the COR within three (3) days of the actual travel date. The travel request shall include the following:

- Contract number
- Date, time, place, and duration of proposed travel
- Purpose of travel and how it relates to the contract
- Travel cost estimate (with complete breakdown of estimated travel and per diem charges)
- Name(s) of individual(s) traveling
- Name of specific government technical POC requesting the travel
- The program/project name that the travel is required for
- Applicable SOW paragraph number
- Total travel funds expended to date
- Balance of authorized travel funding

Trip/activity reports shall be completed and submitted to the COR after completion of the trip. (CDRL A004)

### **6.0 GOVERNMENT FURNISHED PROPERTY/EQUIPMENT**

The Government does not intend to provide GFP on this order.

### **7.0 SECURITY**

The nature of this task requires access to NIWC Pacific databases, contract files that may include proprietary data, Privacy Act data, and unclassified information. The Contractor is required to sign a non-disclosure agreement and comply with the requirements noted in the DD-254. The work performed by the contractor will include access to unclassified and up to Top Secret (TS)/Sensitive Compartmented Information (SCI) data, information, meetings, and spaces. The contractor will be required to provide individuals with up to TS/SCI clearances. Some contractors may come into contact with communications security at Government sites relating to the Secure Internet Protocol Router Network (SIPRNet), Joint Worldwide Intelligence Communications System (JWICS) and Communications Security (COMSEC). The contractor will need access to JWICS in order to view proposal data, assist in the preparation of briefings and technical reports, and communicate with team members.

UNCLASSIFIED

UNCLASSIFIED

Although there is no requirement for the contractor to access NATO on this contract per Naval Intelligence Security Policy Directive 17-008 those contractors that have SCI access and those cleared SCI with JWICS or SIPRnet accounts shall be North Atlantic Treaty Organization (NATO) read-on and complete the derivative classification training prior to being granted access to JWICS/SIPRnet; training is provided by the facility security officer. Specific requirements provided in the Department of Defense Contract Security Classification Specification, DD Form 254.

Contractors performing tasks at the TS or below level without SCI access shall only receive the North Atlantic Treaty Organization (NATO) awareness brief and complete the derivative classification training prior to being granted access to SIPRnet; training is provided by the facility security officer. Specific requirements provided in the Department of Defense Contract Security Classification Specification, DD Form 254.

Contractor personnel assigned to this effort who require access to SCI data and spaces must possess a current SSBI with ICD 704 eligibility (which replaced DCID 6/4 eligibility).

The National Industrial Security Program Operating Manual (NISPOM) 32 CFR NISPOM Rule 117.8 implements contractor reporting requirements per SEAD 3. Contractors are required to report certain events such as those that have an impact on: 1) the status of the facility clearance (FCL), 2) the status of an employee's personnel clearance (PCL); may indicate the employee poses an insider threat the proper, 3) the proper safeguarding of classified information, and 4) or an indication that classified information has been lost or compromised. Contractors working under NIWC Pacific contracts will ensure information pertaining to assigned contractor personnel are reported to the Contracting Officer Representative (COR)/Technical Point of Contact (TPOC), the Contracting Specialist, and the Security's COR in addition to notifying appropriate agencies such as Cognizant Security Agency (CSA), Cognizant Security Office (CSO), or Department Of Defense Central Adjudication Facility (DODCAF) when that information relates to the denial, suspension, or revocation of a security clearance of any assigned personnel; any adverse information on an assigned employee's continued suitability for continued access to classified access; any instance of loss or compromise, or suspected loss or compromise, of classified information; actual, probable or possible espionage, sabotage, or subversive information; or any other circumstances of a security nature that would affect the contractor's operation while working under NIWC Pacific contracts.

If foreign travel is required, all outgoing Country/Theater clearance message requests shall be submitted to the Commanding Officer, Attn: Foreign Travel Team, Naval Information Warfare Center Pacific, 53560 Hull Street Building 27, 2nd Floor -Room 206, San Diego, CA 92152 for action. A Request for Foreign Travel form shall be submitted for each traveler, in advance of the travel, to initiate the release of a clearance message at least 30 days in advance of departure. Each Traveler must also submit a Personal Protection Plan and have a Level 1 Antiterrorism/Force Protection briefing within one year of departure and a country specific

UNCLASSIFIED

UNCLASSIFIED

briefing within 90 days of departure. Anti-Terrorism/Force Protection (AT/FP) briefings are required for all personnel (Military, DOD Civilian, and contractor) per OPNAVINST F3300.53D. Contractor employees must receive the AT/FP briefing annually. The briefing is available at Joint Knowledge Online (JKO): <https://jkodirect.jten.mil> (prefix): JS; course number: US007; title: Level 1 Anti-terrorism awareness training, if experiencing problems accessing this website contact the JKO Help Desk (24 hours a day/7 days a week, <https://jkodirect.jten.mil>, 757-203-5654). This training can also be found on the Total Workforce Management Services (TWMS) site: <https://twms.navy.mil/selfservice>. Sere 100.2 Level A code of conduct training is also required prior to Oconus travel for all personnel. Sere 100.2 Level A training can be accessed <https://jkodirect.jten.mil/Atlas2/page/desktop/DesktopHome.jsf>, recommend course: prefix: J3T: course #: A-US1329, for civilian, military, and contractors. Personnel utilizing the JKO site must have a CAC or contractor shall request a sponsored account to access the training. NOTE: Please email or fax the certificate to Foreign Travel Group (ssc\_fortrav@navy.mil). Other specialized training for specific locations may also be required contact the NIWC Pacific foreign travel team at (ssc\_fortrav@navy.mil). Additional information can be found in NIWC PACINST 4650.3B-Ch-1, dtd 20 February 2019. If you have questions about the process contact your NIWC Pacific COR.

Finally, EUCOM has mandated that all personnel going on official travel to the EUCOM AOR must now register with the Smart Traveler Enrollment Program (STEP). When you sign up, you will automatically receive the most current information the State Department compiles about your destination country. You will also receive updates, including Travel Warnings and Travel Alerts. Sign up is one-time only, after you have established your STEP account, you can easily add official or personal travel to anywhere in the world, not just EUCOM.

<http://travel.state.gov/content/passports/en/go/step.html>

<http://travel.state.gov/content/passports/en/go/step.html>.

**7.1 Operations Security (OPSEC).** OPSEC is a five step analytical process (identify critical information; analyze the threat; analyze vulnerabilities; assess risk; develop countermeasures) that is used as a means to identify, control, and protect unclassified and unclassified sensitive information associated with U.S. national security related programs and activities. All personnel working under this task will at some time handle, produce or process command(s) Critical Information or Critical Program Information, and therefore all Contractor personnel must practice OPSEC. All work is to be performed in accordance with DoD OPSEC requirements, and in accordance with the OPSEC attachment to the DD-254.

UNCLASSIFIED

**7.1.1 Operations Security (OPSEC) Requirements.** Security programs are oriented towards protection of classified information and material. Operations Security (OPSEC) is an operations function, which involves the protection of any critical information – focusing on unclassified information that may be susceptible to adversary exploitation. Pursuant to DoDD 5205.02E SECNAVINST 3070.2A, and NAVWARINST 3432.1, NAVWAR/NIWC Atlantic/NIWC Pacific's OPSEC program implements requirements in DoD 5205.02-M – OPSEC Program Manual. Note: OPSEC requirements are applicable when contract personnel have access to classified information, unclassified Critical Program Information (CPI), Controlled Unclassified Information (CUI) or Department of Navy (DoN) networks.

**7.1.2 Local and Internal OPSEC Requirement.** Contractor personnel, including subcontractors if applicable, shall adhere to the OPSEC program policies and practices as cited in the NAVWARINST 3432.1 and existing local site OPSEC procedures. The Contractor shall develop their own internal OPSEC program specific to the contract and based on NAVWAR/NIWC Atlantic/NIWC Pacific OPSEC requirements. The Contractor's program shall identify the current contractor site OPSEC Officer/Coordinator/POC.

**7.1.3 OPSEC Training.** Contractor shall track and ensure applicable personnel receive initial and annual OPSEC awareness training. Training may be provided by the government or by the contractor's OPSEC Manager. Contractor training shall include, at a minimum, cover OPSEC as it relates to contract work; discuss the Critical Information applicable in the contract; applicable review of government Critical Information and Indicators List(s) (CIIL); social media awareness and vulnerabilities; local threats; how to protect, transmit, and destroy controlled unclassified information; risks and guidance pertaining to geolocation-capable devices, applications, and services; and OPSEC review procedures for public release. The Contractor shall ensure that training materials developed by the Contractor shall be reviewed by the NAVWAR/NIWC Atlantic/NIWC Pacific OPSEC Officer, who will ensure it is consistent with NAVWAR/NIWC Atlantic/NIWC Pacific OPSEC policies. OPSEC training requirements are applicable for personnel during their entire term supporting NAVWAR/NIWC Atlantic/NIWC Pacific contracts and for the duration of DoN network access.

**7.1.4 NAVWAR/NIWC Atlantic/NIWC Pacific OPSEC Program.** If required, the Contractor shall participate in NAVWAR/NIWC Atlantic/NIWC Pacific OPSEC program briefings and working meetings, and complete any required OPSEC survey or data call within the timeframe specified.

**7.2 Contractor Requirements for Intelligence Oversight.** In compliance with DoDD 5148.13 paragraph 4.1.e and SECNAVINST 3820.3F, all contractor personnel conducting Intelligence or Intelligence-related activities or supporting those efforts under Department of Defense authorities shall report any Questionable Intelligence Activity (QIA) or Significant or Highly Sensitive Matter (S/HSM) to the Naval Information Warfare Systems Command Intelligence Oversight Program Manager or Senior Intelligence Officer.

**7.2.1 Questionable Intelligence Activity (QIA):** Any Intelligence or Intelligence-related activity when there is reason to believe such activity may be unlawful or contrary to an Executive Order, Presidential Directive, Intelligence Community Directive, or applicable DoD policy governing that activity.

**7.2.2 Significant or Highly Sensitive Matter (S/HSM):** An Intelligence or Intelligence-related activity (regardless of whether the Intelligence or Intelligence-related activity is unlawful or contrary to an Executive Order, Presidential Directive, Intelligence Community Directive, or DoD policy), or serious criminal activity by Intelligence personnel, that could impugn the reputation or integrity of the Intelligence Community, or otherwise call into question the propriety of Intelligence activities. Such matters might involve actual or potential:

- Congressional inquiries or investigations.
- Adverse media coverage.
- Impact on foreign relations or foreign partners.
- Systemic compromise, loss, or unauthorized disclosure of protected information.

## **8.0 OTHER**

- 8.1 *Deliverables.* The Contractor shall provide the deliverables listed in the Contracts Data Requirements List (CDRL), Exhibit A Contracts Data Requirements List DD Form 1423. Deliverables shall be prepared in contractor format where not otherwise specified by the Government.
- 8.2 *Workstations.* Navy/Marine Corps Intranet (NMCI) seats will be available for contractors working on site. The Government will provide desk space and administrative/office supplies to on-site contractor support personnel.
- 8.3 The Government will provide property, information, and/or material for the performance of this SOW including NMCI CACs, alternate tokens, and SIPRnet tokens as required. The Contractor PM/FSO is responsible for notifying the Government COR and the Trusted Agent (TA) when an employee who has been issued a CAC leaves the Company or transfers to another Program/Project. In the case of an employee who no longer works for the Company, the Company must collect the CAC and surrender it to the COR within two (2) working days of the employee's departure. In the case of an employee still retained by the company transferring to another Program/Project within NAVWAR, the company will notify the COR within two (2) working days so the TA can transfer the TA responsibilities to the new TA vice revoking and issuing a new CAC. Alternate tokens and SIPRNet tokens shall be surrendered upon departure to the Local Registration Authority (LRA) first, and if not available, to the COR.

UNCLASSIFIED

CDRL	SOW Para.	Title
A001	3.1-3.4 3.5.1 3.6-3.10	Contractor's Progress and Status Report
A002	3.1-3.10	Technical Report
A003	3.1-3.10	Briefings, Spreadsheets, and Training Reports
A004	5.0	Trip/Travel Report

## 9.0 PERFORMANCE REQUIREMENTS SUMMARY

9.1 *Performance Objective.* The contractor shall provide services and deliverables in accordance with this SOW and in accordance with the attached task order Contract Data Requirements List (CDRL) items.

9.2 *Performance Standard.* The contractor's performance shall meet all of the requirements of this SOW and comply with all applicable guidance, directives, and standards. The contractor shall deliver all task order data items in accordance with the authorities, content, format, media, marking, applications, quantities, frequency and submission date, delivery method, addressee, and DD-250 requirements specified in the CDRL for each data item.

9.3 *Acceptable Quality Level.* The effectiveness of the contractor's deliverables and services will be measured for 99% compliance with all SOW and CDRL requirements. The Government will evaluate (1) the quality of services and deliverables in terms of the contractor's compliance with the performance standard, (2) the contractors' timeliness with respect to task order, milestones, and delivery schedules, (3) the contractor's cost control in terms of effectiveness in forecasting, managing, and controlling cost, and (4) the contractor's business relations in terms of timeliness, completeness, quality of problem identification and corrective action, and reasonable and cooperative behavior.

## SOW Addendum

### I. NIWC PACIFIC WORK WEEK

(a) All or a portion of the effort under this contract will be performed on a Government installation. The normal work week for Government employees at NIWC Pacific is Monday through Thursday 7:15 AM to 4:45 PM and Friday 7:15 AM to 3:45 PM with every other Friday a non-work day. Work at this Government installation, shall be performed by the contractor within the normal work

UNCLASSIFIED

UNCLASSIFIED

hours at NIWC Pacific unless differing hours are specified on an individual delivery/task order. The contractor is not required to maintain the same hours as Government employees; however, contractor employees performing work at NIWC Pacific must work during the normal workweek. The following is a list of holidays observed by the Government.

<u>Name of Holiday</u>	<u>Time of Observance</u>
New Year's Day	1 January
Martin Luther King Jr. Day	Third Monday in January
Presidents Day	Third Monday in February
Memorial Day	Last Monday in May
Juneteenth National Independence Day	19 June
Independence Day	4 July
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veteran's Day	11 November
Thanksgiving Day	Fourth Thursday in November
Christmas Day	25 December

(b) If any of the above holidays occur on a Saturday or a Sunday, then such holiday shall be observed by the contractor in accordance with the practice as observed by the assigned Government employees at the using activity.

(c) If the contractor is prevented from performance as the result of an Executive Order or an administrative leave determination applying to the using activity, such time may be charged to the contract as direct cost provided such charges are consistent with the contractor's accounting practices.

(d) This contract does not allow for payment of overtime during the normal workweek for employees who are not exempted from the Fair Labor Standards Act unless expressly authorized by the Ordering Officer. Under Federal regulations, the payment of overtime is required only when an employee works more than 40 hours during a week. Therefore, during the NIWC Pacific off-Friday (36-hour) week overtime will not be paid for non-exempt employees. During the work-Friday week (44 hour) the contractor is to schedule work so as not to incur overtime charges during the normal work week unless authorized in writing by the Government to do so. An example of this would be for contractor personnel to work during the hours of 7:15 AM to 4:45 PM Monday through Thursday and 7:15 AM to 3:45 PM Friday during the work-Friday week. The contractor may also elect to configure the workforce in such a way that no single employee exceeds 40 hours during a normal week even though normal NIWC Pacific hours are maintained both weeks.

(e) NOTICE: All contractor employees who make repeated deliveries to military installations shall obtain the required employee pass via the Defense Biometric Identification System (DBIDS) in order to gain access to the facility. Information about DBIDS may be found at the following website: <https://www.cniv.navy.mil/om/dbids.html>.

UNCLASSIFIED

## UNCLASSIFIED

Contractor employees must be able to obtain a DBIDS in accordance with base security requirements. Each employee shall wear the Government issued DBIDS badge over the front of the outer clothing. When an employee leaves the contractor's employ, the employee's DBIDS badge shall be returned to the Contracting Officer's Representative or the base Badge and Pass Office within five (5) calendar days.

Contractors who do not have a DBIDS or Common Access Card (CAC) must be issued a one-day pass daily at the Badge and Pass Office. Issuance of a CAC requires the need for physical access to the installation and logical access to government owned computer systems.

(f) Periodically, the Government may conduct Anti-Terrorism Force Protection (AT/FP) and/or safety security exercises, which may require the contractor to adjust its work schedule and/or place of performance to accommodate execution of the exercise. The contractor will be required to work with its Government point of contact to adjust work schedules and/or place of performance in the case of an exercise that causes disruption of normally scheduled work hours or disruption of access to a government facility. The contract does not allow for payment of work if schedules cannot be adjusted and/or the work cannot be executed remotely (i.e., the contractor's facility or alternate non-impacted location), during an exercise when government facilities are inaccessible.

## **II. LIABILITY INSURANCE--COST TYPE CONTRACTS**

(a) The following types of insurance are required in accordance with FAR 52.228-7 "Insurance--Liability to Third Persons" and shall be maintained in the minimum amounts shown:

(1) Workers' compensation and employers' liability: minimum of \$100,000

(2) Comprehensive general liability: \$500,000 per occurrence

(3) Automobile liability: \$200,000 per person

\$500,000 per occurrence

\$ 20,000 per occurrence for property damage

(b) When requested by the contracting officer, the contractor shall furnish to the Contracting Officer a certificate or written statement of insurance. The written statement of insurance must contain the following information: policy number, policyholder, carrier, amount of coverage, dates of effectiveness (i.e., performance period), and contract number. The contract number shall be cited on the certificate of insurance.

## **III. KEY PERSONNEL**

UNCLASSIFIED

UNCLASSIFIED

(a) The offeror agrees to assign to this contract those key personnel listed in paragraph (d) below. No substitutions shall be made except in accordance with this text.

(b) The offeror agrees that during the first 180 days of the contract performance period no personnel substitutions will be permitted unless such substitutions are necessitated by an individual's sudden illness, death or termination of employment. In any of these events, the contractor shall promptly notify the Contracting Officer and provide the information required by paragraph (c) below. After the initial 180 day period, all proposed substitutions must be submitted in writing, at least fifteen (15) days (thirty (30) days if a security clearance is to be obtained) in advance of the proposed substitutions to the contracting officer. These substitution requests shall provide the information required by paragraph (c) below.

(c) All requests for approval of substitutions under this contract must be in writing and provide a detailed explanation of the circumstances necessitating the proposed substitutions. They must contain a complete resume for the proposed substitute or addition, and any other information requested by the Contracting Officer or needed by him to approve or disapprove the proposed substitutions. All substitutions proposed during the duration of this contract must have qualifications of the person being replaced. The Contracting Officer or authorized representative will evaluate such requests and promptly notify the contractor of approval or disapproval thereof in writing.

(d) List of Key Personnel

NAME

(b)4

CONTRACT LABOR CATEGORY

Program Manager – Level III

Data Analyst – Level III -SOW paragraph 3.2 - 3.7

Data Analyst – Level III - SOW paragraph 3.9

(e) If the Contracting Officer determines that suitable and timely replacement of key personnel who have been reassigned, terminated or have otherwise become unavailable for the contract work is not reasonably forthcoming or that the resultant reduction of productive effort would be so substantial as to impair the successful completion of the contract or the service order, the contract may be terminated by the Contracting Officer for default or for the convenience of the Government, as appropriate. In addition, if the contractor is found at fault for the condition, the Contracting Officer may elect to equitably decrease the contract price or fixed fee to compensate the Government for any resultant delay, loss or damage.

(f) If the offeror wishes to add personnel to be used in a labor category, it shall employ the procedures outlined in paragraph (c) above. Adding personnel will only be permitted in the event of an indefinite quantity contract, where the Government has issued a delivery order for labor hours that would exceed a normal forty hour week if performed only by the number of employees originally proposed.

UNCLASSIFIED

#### **IV. CONTRACTOR IDENTIFICATION**

- (a) Contractor employees must be clearly identifiable while on Government property by wearing appropriate badges.
- (b) Contractor personnel and their subcontractors must identify themselves as contractors or subcontractors during meetings, telephone conversations, in electronic messages, or correspondence related to this contract.
- (c) Contractor-occupied facilities (on Department of the Navy or other Government installations) such as offices, separate rooms, or cubicles must be clearly identified with contractor supplied signs, name plates or other identification, showing that these are work areas for contractor or subcontractor personnel.

#### **V. REIMBURSEMENT OF TRAVEL COSTS**

##### **(a) Contractor Request and Government Approval of Travel**

Any travel under this contract must be specifically requested in writing, by the contractor prior to incurring any travel costs. If this contract is an indefinite-delivery contract, then the written Government authorization will be by task/delivery orders issued by the Ordering Officer or by a modification to an issued task/delivery order. If this contract is an indefinite-delivery contract, then the written Government authorization will be by written notice of approval from the Contracting Officer's Representative (COR). The request shall, at a minimum, include:

- (1) Contract number
- (2) Date, time, and place of proposed travel
- (3) Purpose of travel and how it relates to the contract
- (4) Contractor's estimated cost of travel
- (5) Name(s) of individual(s) traveling and;
- (6) A breakdown of estimated travel and per diem charges.

##### **(b) General**

(1) The costs for travel, subsistence, and lodging shall be reimbursed to the contractor only to the extent that it is necessary and authorized for performance of the work under this contract. The costs for travel, subsistence, and lodging shall be reimbursed to the contractor in accordance with the Federal Acquisition Regulation (FAR) 31.205-46, which is incorporated by reference into this contract. As specified in FAR 31.205-46(a) (2), reimbursement for the costs incurred for lodging, meals and incidental expenses (as defined in the travel regulations cited subparagraphs (b)(1)(i) through (b)(1)(iii) below) shall be considered to be reasonable and allowable only to the extent that they do not exceed on a daily basis the maximum per diem rates in effect at the time of travel as set forth in the following:

UNCLASSIFIED

(i) Federal Travel Regulation prescribed by the General Services Administration for travel in the contiguous 48 United States;

(ii) Joint Travel Regulation, Volume 2, DoD Civilian Personnel, Appendix A, prescribed by the Department of Defense for travel in Alaska, Hawaii, The Commonwealth of Puerto Rico, and the territories and possessions of the United States; or

(iii) Standardized Regulations, (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances in Foreign Areas" prescribed by the Department of State, for travel in areas not covered in the travel regulations cited in subparagraphs (b)(1)(i) and (b)(1)(ii) above.

(2) Personnel in travel status from and to the contractor's place of business and designated work site or vice versa, shall be considered to be performing work under the contract, and contractor shall bill such travel time at the straight (regular) time rate; however, such billing shall not exceed eight hours per person for any one person while in travel status during one calendar day.

(c) Per Diem

(1) The contractor shall not be paid per diem for contractor personnel who reside in the metropolitan area in which the tasks are being performed. Per diem shall not be paid on services performed at contractor's home facility and at any facility required by the contract, or at any location within a radius of 50 miles from the contractor's home facility and any facility required by this contract.

(2) Costs for subsistence and lodging shall be paid to the contractor only to the extent that overnight stay is necessary and authorized in writing by the Government for performance of the work under this contract per paragraph (a). When authorized, per diem shall be paid by the contractor to its employees at a rate not to exceed the rate specified in the travel regulations cited in FAR 31.205-46(a)(2) and authorized in writing by the Government. The authorized per diem rate shall be the same as the prevailing locality per diem rate.

(3) Reimbursement to the contractor for per diem shall be limited to payments to employees not to exceed the authorized per diem and as authorized in writing by the Government per paragraph (a). Fractional parts of a day shall be payable on a prorated basis for purposes of billing for per diem charges attributed to subsistence on days of travel. The departure day from the Permanent Duty Station (PDS) and return day to the PDS shall be 75% of the applicable per diem rate. The contractor shall retain supporting documentation for per diem paid to employees as evidence of actual payments.

(d) Transportation

(1) The contractor shall be paid on the basis of actual amounts paid to the extent that such transportation is necessary for the performance of work under the contract and is authorized in writing by the Government per paragraph (a).

UNCLASSIFIED

UNCLASSIFIED

(2) The contractor agrees, in the performance of necessary travel, to use the lowest cost mode commensurate with the requirements of the mission and in accordance with good traffic management principles. When it is necessary to use air or rail travel, the contractor agrees to use coach, tourist class or similar accommodations to the extent consistent with the successful and economical accomplishment of the mission for which the travel is being performed. Documentation must be provided to substantiate non-availability of coach or tourist if business or first class is proposed to accomplish travel requirements.

(3) When transportation by privately owned conveyance (POC) is authorized, the contractor shall be paid on a mileage basis not to exceed the applicable Government transportation rate specified in the travel regulations cited in FAR 31.205-46(a)(2) and is authorized in writing by the Government per paragraph (a).

(4) When transportation by privately owned (motor) vehicle (POV) is authorized, required travel of contractor personnel, that is not commuting travel, may be paid to the extent that it exceeds the normal commuting mileage of such employee. When an employee's POV is used for travel between an employee's residence or the Permanent Duty Station and one or more alternate work sites within the local area, the employee shall be paid mileage for the distance that exceeds the employee's commuting distance.

(5) When transportation by a rental automobile, other special conveyance or public conveyance is authorized, the contractor shall be paid the rental and/or hiring charge and operating expenses incurred on official business (if not included in the rental or hiring charge). When the operating expenses are included in the rental or hiring charge, there should be a record of those expenses available to submit with the receipt. Examples of such operating expenses include hiring charge (bus, streetcar or subway fares), gasoline and oil, parking, and tunnel tolls.

(6) Definitions:

(i) "Permanent Duty Station" (PDS) is the location of the employee's permanent work assignment (i.e., the building or other place where the employee regularly reports for work.

(ii) "Privately Owned Conveyance" (POC) is any transportation mode used for the movement of persons from place to place, other than a Government conveyance or common carrier, including a conveyance loaned for a charge to, or rented at personal expense by, an employee for transportation while on travel when such rental conveyance has not been authorized/approved as a Special Conveyance.

(iii) "Privately Owned (Motor) Vehicle (POV)" is any motor vehicle (including an automobile, light truck, van or pickup truck) owned by, or on a long-term lease (12 or more months) to, an employee or that employee's dependent for the primary purpose of providing personal transportation, that:

- (a) is self-propelled and licensed to travel on the public highways;
- (b) is designed to carry passengers or goods; and

UNCLASSIFIED

UNCLASSIFIED

(c) has four or more wheels or is a motorcycle or moped.

(iv) “Special Conveyance” is commercially rented or hired vehicles other than a POC and other than those owned or under contract to an agency.

(v) “Public Conveyance” is local public transportation (e.g., bus, streetcar, subway, etc.) or taxicab.

(iv) “Residence” is the fixed or permanent domicile of a person that can be reasonably justified as a bona fide residence.

EXAMPLE 1: Employee’s one way commuting distance to regular place of work is 7 miles. Employee drives from residence to an alternate work site, a distance of 18 miles. Upon completion of work, employee returns to residence, a distance of 18 miles.

In this case, the employee is entitled to be reimbursed for the distance that exceeds the normal round trip commuting distance (14 miles). The employee is reimbursed for 22 miles ( $18 + 18 - 14 = 22$ ).

EXAMPLE 2: Employee’s one way commuting distance to regular place of work is 15 miles. Employee drives from residence to an alternate work site, a distance of 5 miles. Upon completion of work, employee returns to residence, a distance of 5 miles.

In this case, the employee is not entitled to be reimbursed for the travel performed (10 miles), since the distance traveled is less than the commuting distance (30 miles) to the regular place of work.

EXAMPLE 3: Employee’s one way commuting distance to regular place of work is 15 miles. Employee drives to regular place of work. Employee is required to travel to an alternate work site, a distance of 30 miles. Upon completion of work, employee returns to residence, a distance of 15 miles.

In this case, the employee is entitled to be reimbursed for the distance that exceeds the normal round trip commuting distance (30 miles). The employee is reimbursed for 30 miles ( $15 + 30 + 15 - 30 = 30$ ).

EXAMPLE 4: Employee’s one way commuting distance to regular place of work is 12 miles. In the morning, the employee drives to an alternate work site (45 miles). In the afternoon, the employee returns to the regular place of work (67 miles). After completion of work, employee returns to residence, a distance of 12 miles.

In this case, the employee is entitled to be reimbursed for the distance that exceeds the normal round trip commuting distance (24 miles). The employee is reimbursed for 100 miles ( $45 + 67 + 12 - 24 = 100$ ).

UNCLASSIFIED

UNCLASSIFIED

EXAMPLE 5: Employee's one way commuting distance to regular place of work is 35 miles. Employee drives to the regular place of work (35 miles). Later, the employee drives to alternate work site #1 (50 miles) and then to alternate work site #2 (25 miles). Employee then drives to residence (10 miles).

In this case, the employee is entitled to be reimbursed for the distance that exceeds the normal commuting distance (70 miles). The employee is reimbursed for 50 miles ( $35 + 50 + 25 + 10 - 70 = 50$ ).

EXAMPLE 6: Employee's one way commuting distance to regular place of work is 20 miles. Employee drives to the regular place of work (20 miles). Later, the employee drives to alternate work site #1 (10 miles) and then to alternate work site #2 (5 miles). Employee then drives to residence (2 miles).

In this case, the employee is not entitled to be reimbursed for the travel performed (37 miles), since the distance traveled is less than the commuting distance (40 miles) to the regular place of work.

**VI. DESIGNATION OF CONTRACTING OFFICER'S REPRESENTATIVE**

The Contracting Officer hereby appoints the following individuals as Contracting Officer's Representative (COR) for this contract/order:

Name: Lauryn Hiser  
Code: 72110  
Phone Number: 619-553-0905  
E-mail: [lauryn.a.hiser.civ@us.navy.mil](mailto:lauryn.a.hiser.civ@us.navy.mil)

Name: Ryan Lu (TS/SCI COR)  
Code: 72110  
Phone Number: 619- 767-4172  
E-mail: [ryan.p.lu.civ@us.navy.mil](mailto:ryan.p.lu.civ@us.navy.mil)

**VII. REQUIRED INFORMATION ASSURANCE AND PERSONNEL SECURITY REQUIREMENTS FOR ACCESSING GOVERNMENT INFORMATION SYSTEMS AND NONPUBLIC INFORMATION**

Definition. As used in this text, "sensitive information" includes:

All types and forms of confidential business information, including financial information relating to a contractor's pricing, rates, or costs, and program information relating to current or estimated budgets or schedules;

Source selection information, including bid and proposal information as defined in FAR 2.101 and FAR 3.104-4, and other information prohibited from disclosure by the Procurement Integrity Act (41 USC 423);

UNCLASSIFIED

UNCLASSIFIED

Information properly marked as “business confidential,” “proprietary,” “procurement sensitive,” “source selection sensitive,” or other similar markings;  
Other information designated as sensitive by the Naval Information Warfare Systems Command (NAVWAR).

In the performance of the contract, the contractor may receive or have access to information, including information in Government information systems and secure websites. Accessed information may include “sensitive information” or other information not previously made available to the public that would be competitively useful on current or future related procurements.

Contractors are obligated to protect and safeguard from unauthorized disclosure all sensitive information to which they receive access in the performance of the contract, whether the information comes from the Government or from third parties. The contractor shall—  
Utilize accessed information and limit access to authorized users only for the purposes of performing the services as required by the contract, and not for any other purpose unless authorized;

Safeguard accessed information from unauthorized use and disclosure, and not discuss, divulge, or disclose any accessed information to any person or entity except those persons authorized to receive the information as required by the contract or as authorized by Federal statute, law, or regulation;

Inform authorized users requiring access in the performance of the contract regarding their obligation to utilize information only for the purposes specified in the contract and to safeguard information from unauthorized use and disclosure.

Execute a “Contractor Access to Information Non-Disclosure Agreement,” and obtain and submit to the Contracting Officer a signed “Contractor Employee Access to Information Non-Disclosure Agreement” for each employee prior to assignment;

Notify the Contracting Officer in writing of any violation of the requirements in (i) through (iv) above as soon as the violation is identified, no later than 24 hours. The notice shall include a description of the violation and the proposed actions to be taken, and shall include the business organization, other entity, or individual to whom the information was divulged.

In the event that the contractor inadvertently accesses or receives any information marked as “proprietary,” “procurement sensitive,” or “source selection sensitive,” or that, even if not properly marked otherwise indicates the contractor may not be authorized to access such information, the contractor shall (i) notify the Contracting Officer; and (ii) refrain from any further access until authorized in writing by the Contracting Officer.

The requirements of this text are in addition to any existing or subsequent Organizational Conflicts of Interest (OCI) requirements which may also be included in the contract, and are in addition to any personnel security or Information Assurance requirements, including

UNCLASSIFIED

UNCLASSIFIED

Systems Authorization Access Request (SAAR-N), DD Form 2875, Annual Information Assurance (IA) training certificate, SF85P, or other forms that may be required for access to Government information systems.

Subcontracts. The contractor shall insert paragraphs (a) through (f) of this text in all subcontracts that may require access to sensitive information in the performance of the contract.

Mitigation Plan. If requested by the Contracting Officer, the contractor shall submit, within 45 calendar days following execution of the "Contractor Non-Disclosure Agreement," a mitigation plan for Government approval, which shall be incorporated into the contract. At a minimum, the mitigation plan shall identify the contractor's plan to implement the requirements of paragraph (c) above and shall include the use of a firewall to separate contractor personnel requiring access to information in the performance of the contract from other contractor personnel to ensure that the contractor does not obtain any unfair competitive advantage with respect to any future Government requirements due to unequal access to information. A "firewall" may consist of organizational and physical separation; facility and workspace access restrictions; information system access restrictions; and other data security measures identified, as appropriate. The contractor shall respond promptly to all inquiries regarding the mitigation plan. Failure to resolve any outstanding issues or obtain approval of the mitigation plan within 45 calendar days of its submission may result, at a minimum, in rejection of the plan and removal of any system access.

UNCLASSIFIED